NORTHERN ARIZONA UNIVERSITY

INF639: Nanoelectronics for Cybersecurity

Section 3: Public Key Infrastructure (PKI)

Dr. Bertrand Cambou
Professor of Practice NAU, Cybersecurity
School of Informatics, Computing, and Cyber-Systems
Bertrand.cambou@nau.com

NORTHERN ARIZONA UNIVERSITY

INF 639: Nanoelectronics for cybersecurity

1. From Micro to Nano-electronics
2. Introduction to cryptography
3. Public Key Infrastructure
4. Smartcards
5. Attacks on smartcards
6. MOS transistor & logic circuits
7. Biometry
8. Physical Unclonable Functions (PUF)
9. Access control and authentication
10. Flash Memory devices & security
11. Resistive RAM & security
12. Public key cryptography with PUFs
13. Sensor devices & security
14. Ternary cryptography

NORTHERN ARIZONA UNIVERSITY

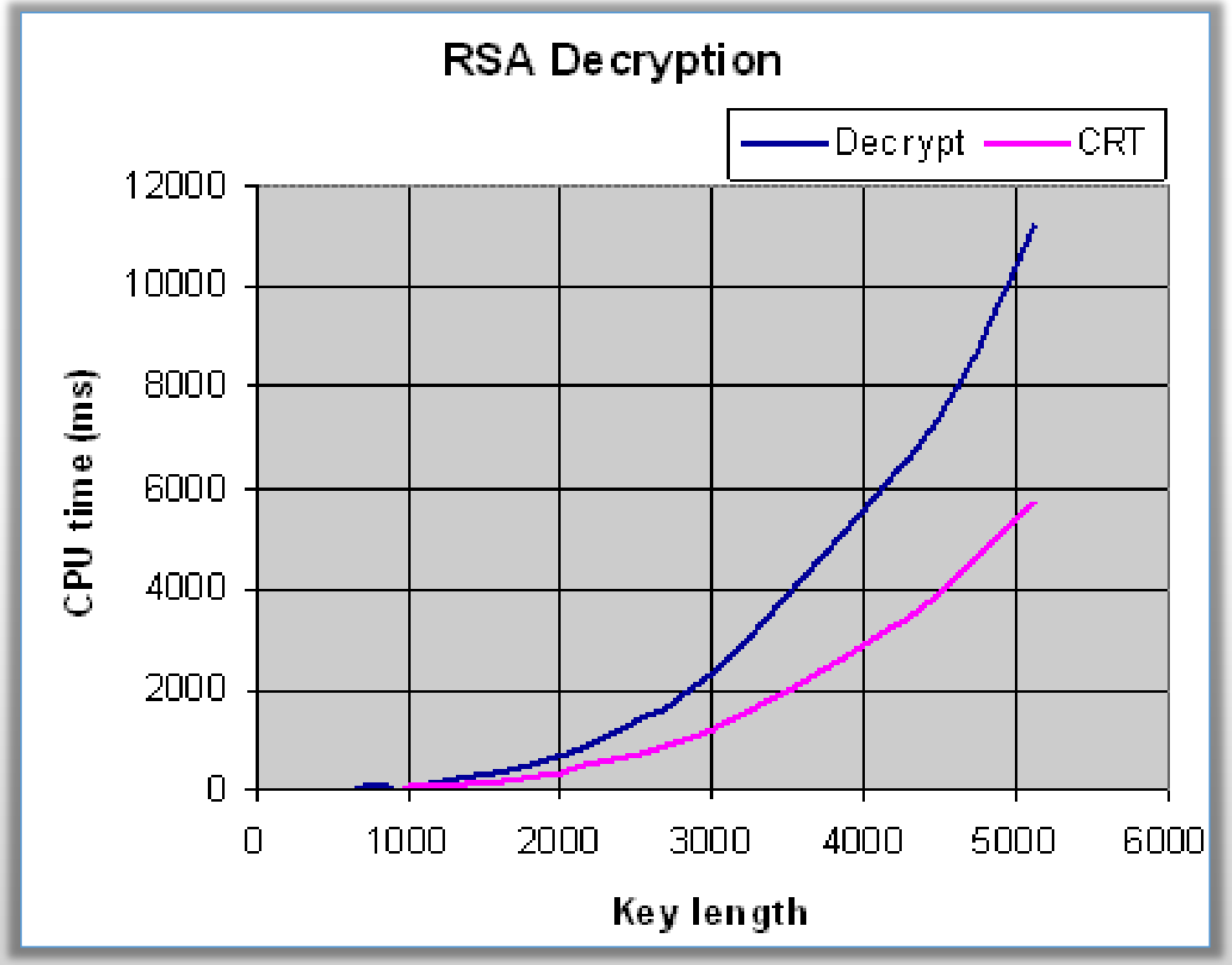
3 Public Key Infrastructure

- 1- Asymmetrical cryptography
- 2- Number theory
- 3- RSA
- 4- ECC

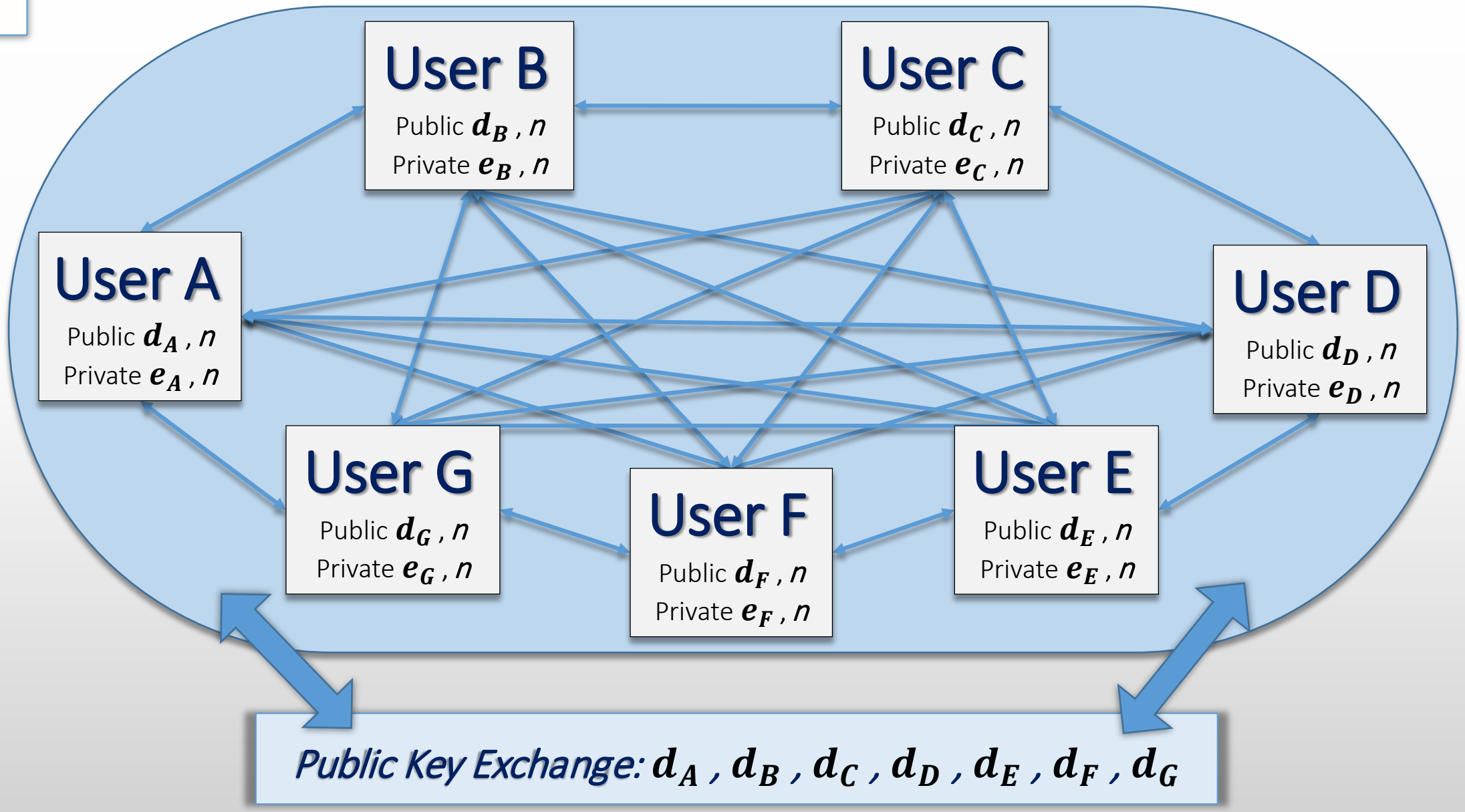
Asymmetrical Cryptography

- Developed by ***Ralph Merkle***, ***Martin Hellman***, ***Whitfield Diffie*** in the early 70's
- Can accommodate a very large number of users operating independently
- RSA: introduced in 1978 (***Ronald Rivest***, ***Adi Shamir***, and ***Leonard Adlemen***)
- Implementation based on the number theory
  - Invert modulo
  - Theorem of Fermat-Euler
- Highly secure, but encryption/decryption slow
- About 1,000 slower than DES/AES
- Typically use 1,000 to 4,000-bit keys
- Existing computers cannot break RSA
- Elliptic curve cryptography (ECC) is more effective
- Quantum cryptography will break both RSA and ECC

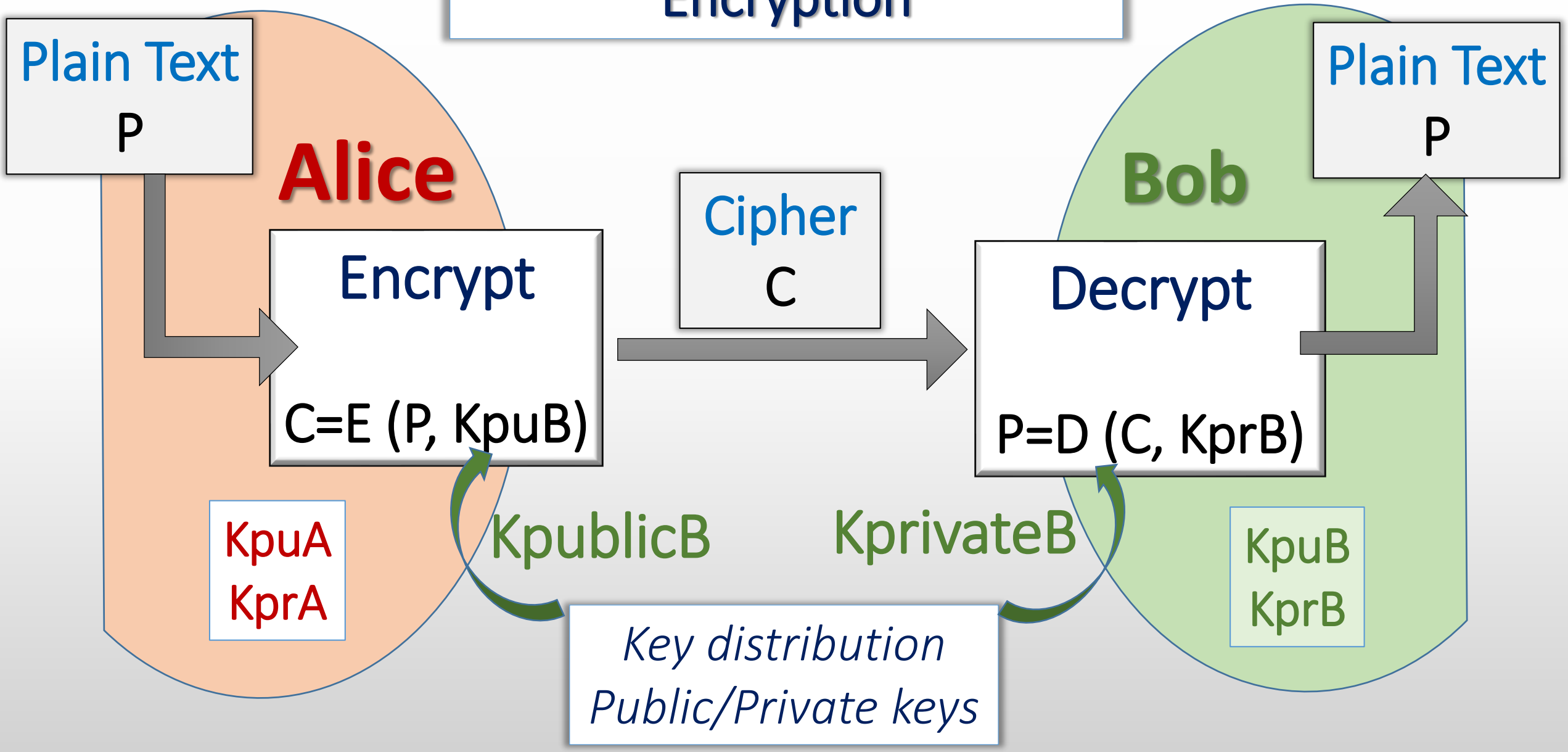
Asymmetrical Cryptography



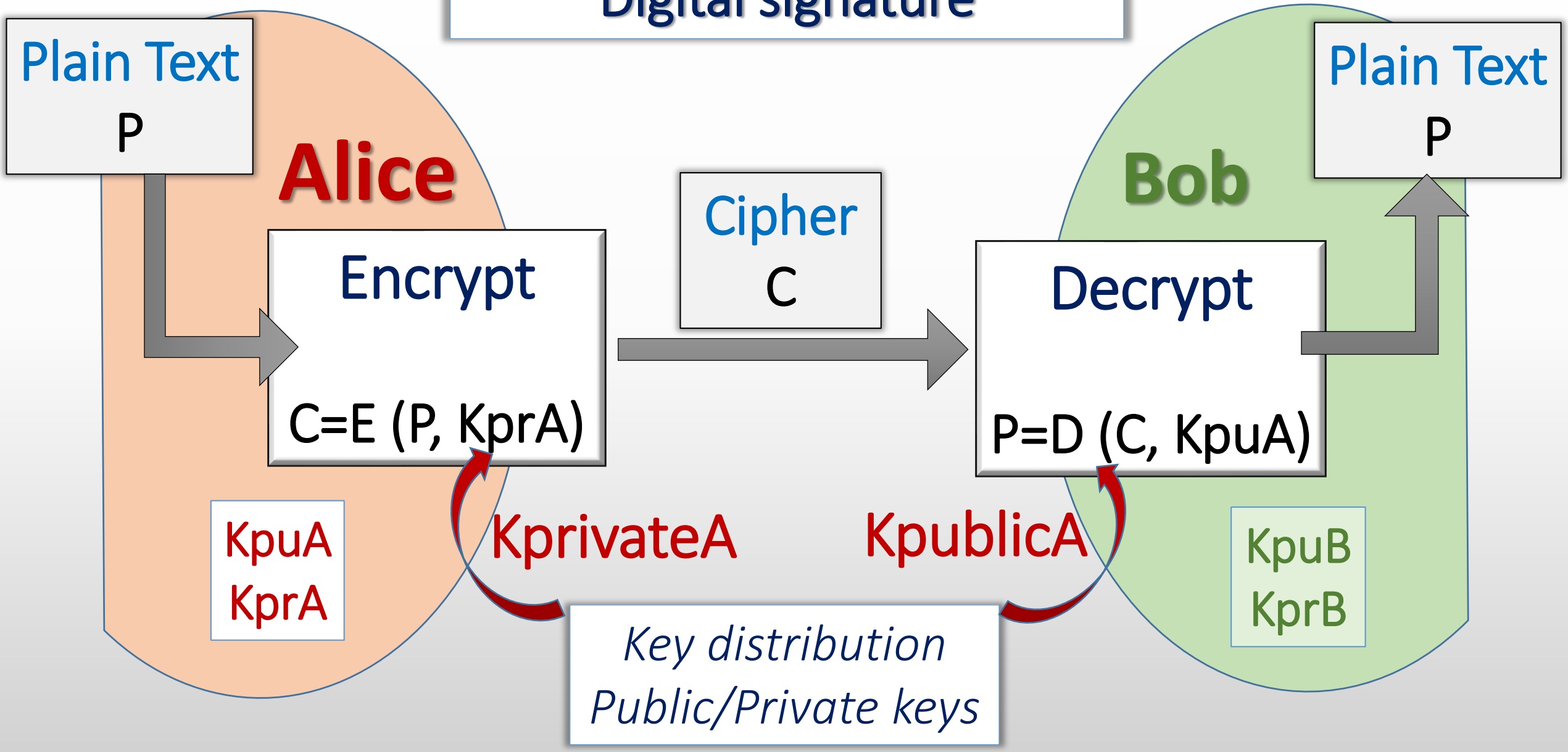
PKI with RSA Key exchange & cryptography



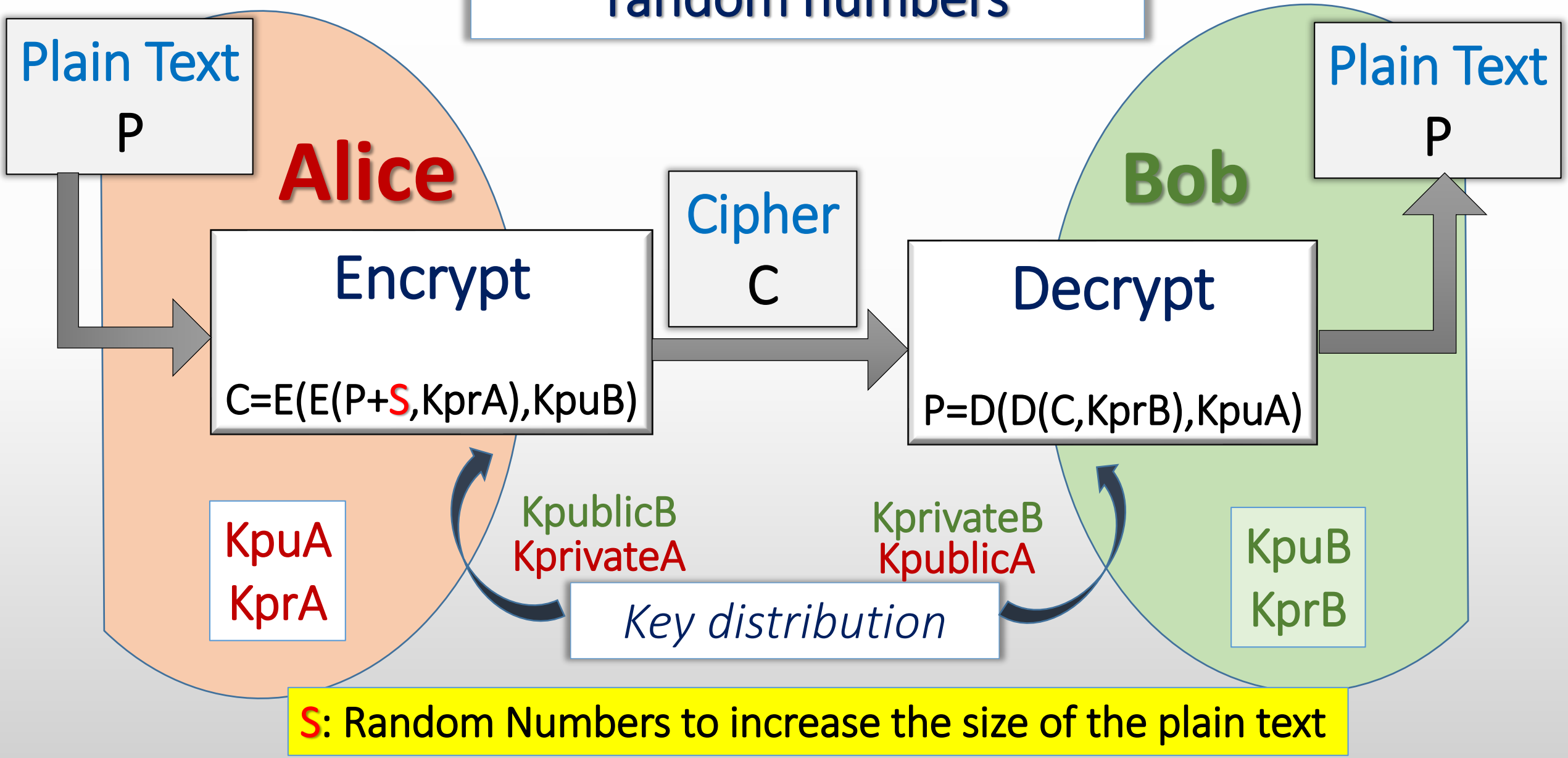
Asymmetrical Cryptography Encryption



Asymmetrical Cryptography
Digital signature



Double Encryption with random numbers



NORTHERN ARIZONA UNIVERSITY

3.Public Key Infrastructure

- 1- Asymmetrical cryptography
- 2- Number theory
- 3- RSA
- 4- ECC

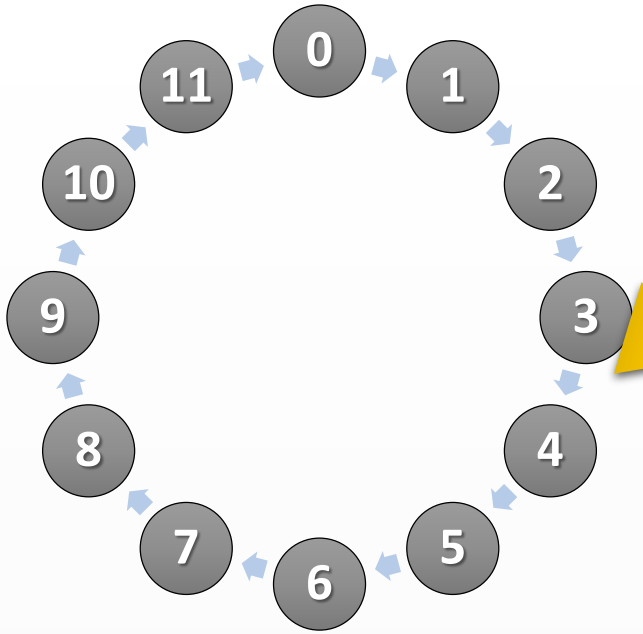
Definition 1

Let $m \neq 0$ be an integer; ***X*** is congruent to ***Y*** modulo ***m***

$$x \bmod(m) = y \quad \text{or} \quad x \equiv y \bmod m$$

if $m \mid (x-y)$, or $\exists$ integer ***k*** such as: $x - y = km$

Class of solutions: $\ldots, y-2m, y-m, y, y+m, y+2m, \ldots$



Example #1: 3 Mod 12 = ?

{ …, -45, -33, -21, -9, 3, 15, 27, 39, 51, ….}

k = -4 -3 -2 -1 0 1 2 3 4

$-45 \equiv 3 \bmod 12$

$39 \equiv 3 \bmod 12$

Basic Arithmetic

Let a, b, c, d, m, n be integers; $m \neq 0$;

$a \bmod(m)=b$ & $c \bmod(m)=d$ then:

(1) $(a + c) \bmod(m) = (b + d)$

(2) $(a - c) \bmod(m) = (b - d)$

(3) $a \times c \bmod(m) = b \times d$

(4) $a^n \bmod(m)=b^n$

Example #2: Modulo 5

$$(13 \times 16) - 8 \equiv X \bmod 5$$

Hard way:

$$(13 \times 16) - 8 = 208 - 8 = 200 \equiv 0 \bmod 5$$

$$X = 0$$

Smart way:

$$(3 \times 1) - 3 = 3 - 3 \equiv 0 \bmod 5$$

Example #3: Modulo 7

Hard way:

$3^8 \bmod 7 = 6561 \bmod 7 = 2$

Smart way:

$3^2 \times 3^2 \times 3^2 \times 3^2 \equiv 2 \times 2 \times 2 \times 2 \bmod 7$

$\equiv (\quad 1 \quad) \times 2 \bmod 7 = 2$

Number Theory: inverse

➢ *Definition 2 (Important for RSA)*

Every $a \in Z_n$, if gcd(n,a)=0,
has a unique multiplicative inverse:

$$a^{-1} \in Z_n \qquad a^{-1}\, a \bmod(m)=1$$

[Ex: for n=14; $3^{-1}= 5$ *(3 x 5 = 14 + 1)*
$9^{-1} = 11$ *(9 x 11 = (14 x 7)+1)*]

Example of prime number - Multiply modulo 19

19	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2	2	4	6	8	10	12	14	16	18	1	3	5	7	9	11	13	15	17
3	3	6	9	12	15	18	2	5	8	11	14	17	1	4	7	10	13	16
4	4	8	12	16	1	5	9	13	17	2	6	10	14	18	3	7	11	15
5	5	10	15	1	6	11	16	2	7	12	17	3	8	13	18	4	9	14
6	6	12	18	5	11	17	4	10	16	3	9	15	2	8	14	1	7	13
7	7	14	2	9	16	4	11	17	6	13	1	8	15	3	10	17	5	12
8	8	16	5	13	2	10	17	6	15	4	12	1	9	17	6	14	3	11
9	9	18	8	17	7	16	6	15	5	14	4	13	3	12	2	11	1	10
10	10	1	11	2	12	3	13	4	14	5	15	6	16	7	17	8	18	9
11	11	3	14	6	17	9	1	12	4	15	7	18	10	2	13	5	16	8
12	12	5	17	10	3	15	8	1	13	6	18	11	4	16	9	2	14	7
13	13	7	1	14	8	2	15	9	3	16	10	4	17	11	5	18	12	6
14	14	9	4	18	13	8	3	17	12	7	2	16	11	6	1	15	10	5
15	15	11	7	3	18	14	10	6	2	17	13	9	5	1	16	12	8	4
16	16	13	10	7	4	1	17	14	11	8	5	2	18	15	12	9	6	3
17	17	15	13	11	9	7	5	3	1	18	16	14	12	10	8	6	4	2
18	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

N	Inv.
1	1
2	10
3	13
4	5
5	4
6	16
7	11
8	12
9	17
10	2
11	7
12	8
13	3
14	15
15	14
16	6
17	9
18	18

Example of composite number: Multiply modulo 15

X 15	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	2	4	6	8	10	12	14	1	3	5	7	9	11	13
3	3	6	9	12	0	3	6	9	12	0	3	6	9	12
4	4	8	12	1	5	9	13	2	6	10	14	3	7	11
5	5	10	0	5	10	0	5	10	0	5	10	0	5	10
6	6	12	3	9	0	6	12	3	9	0	6	12	3	9
7	7	14	6	13	5	12	14	11	3	10	2	9	1	8
8	8	1	9	2	10	3	11	4	12	5	13	6	14	7
9	9	3	12	6	0	9	3	12	6	0	9	3	12	6
10	10	5	0	10	5	0	10	5	0	10	5	0	10	5
11	11	7	3	14	10	6	2	13	9	5	1	12	8	4
12	12	9	6	3	0	12	9	6	3	0	12	9	6	3
13	13	11	9	7	5	3	1	14	12	10	8	6	4	2
14	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Number Theory intercept - 2

➢ *Definition 3: Euler parameter*

For integer n>0 we define: ϕ(n)=number of positive integer lower than n relatively prime to n. [Ex: *n*=15, ϕ(15)=8 *(1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14)*]

If n is prime: ϕ(n)=(n-1)

➢ *Theorem 2*

If *p, q* are primes and ***n=p x q*** then: ϕ(*n*)= ϕ(*p*) x ϕ(*q*)=(*p*-1) x (*q*-1)

➢ *Theorem 3 (little Fermat Theorem)*

Let n be prime, **a<n**, a and n relatively primes, then: $\boldsymbol{a^{n-1} \bmod (n) = 1}$

➢ *Theorem 4 (Euler-Fermat Theorem)*

Let n be prime, ***a<n***, a and n relatively primes, then: $\boldsymbol{a^{\phi(n)} \bmod (n) = 1}$

General form: $\boldsymbol{a^{k\phi(n)+1} \bmod (n) = a}$)

NORTHERN ARIZONA UNIVERSITY

Public Key Infrastructure

- 1- Asymmetrical cryptography
- 2- Number theory
- 3- RSA
- 4- ECC

RSA: Key generation

1- *Select* p & q (typ. = 1000bits) p and q are prime, $p \neq q$

2- *Calculate* n : $n = p \times q$

3- *Calculate* $\phi(n)$: $\phi(n) = (p-1)(q-1)$

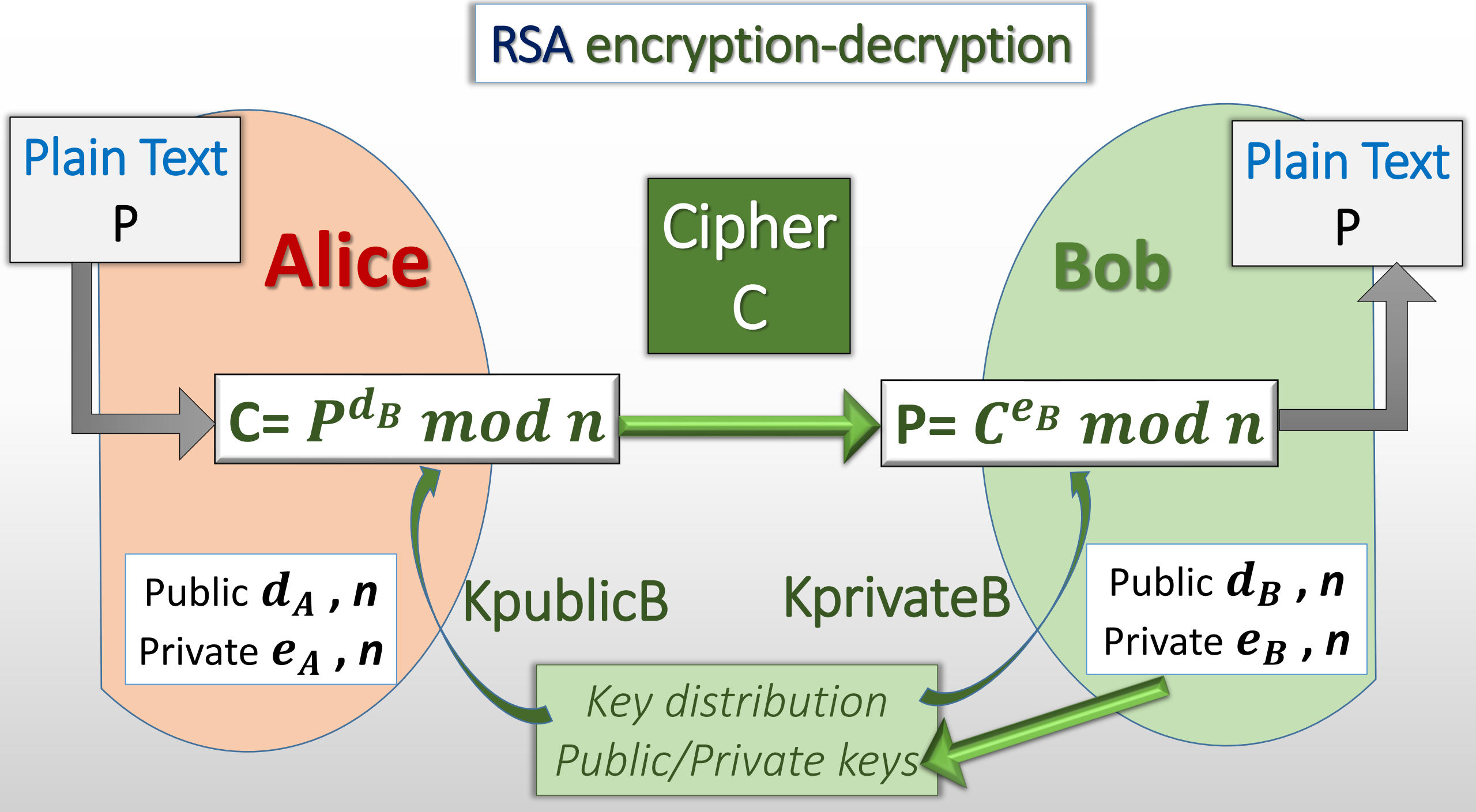
4- *Select integer* e : $gcd(\phi(n), e) = 1$; $e \in \{1, 2, \ldots, \phi(n)-1\}$

5- *Calculate* d : $d \times e \equiv 1 \bmod \phi(n)$ Use EEA

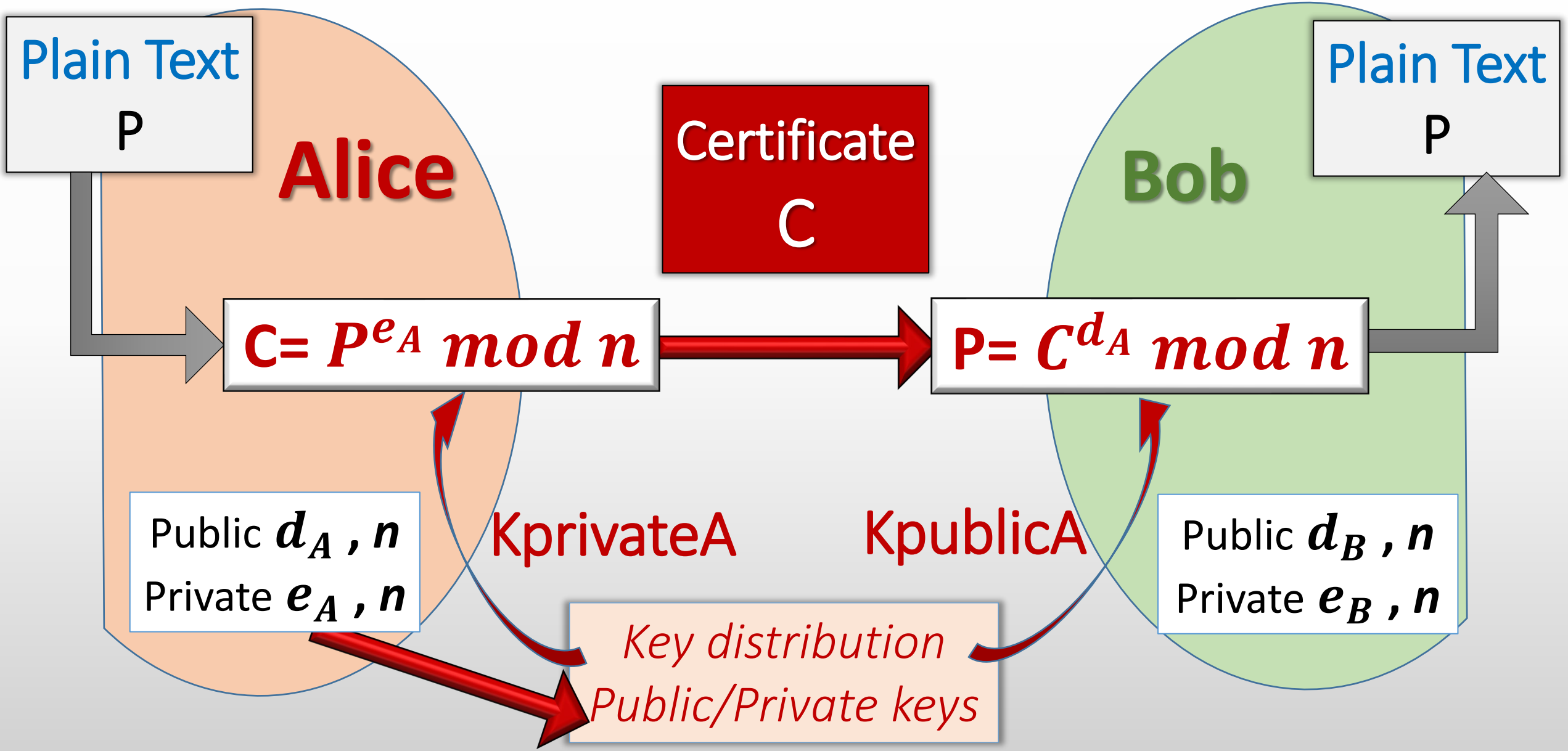
Public Key ➔ $Kpub = \{e, n\}$

Private Key ➔ $Kpriv = \{d, n\}$

➔ $\phi(n)$ is kept secret


RSA encryption-decryption
Plain Text
P
Alice
Cipher
C
Bob
Plain Text
P
C= $P^{d_B}\ mod\ n$
P= $C^{e_B}\ mod\ n$
Public d_A , n
Private e_A , n
KpublicB
KprivateB
Public d_B , n
Private e_B , n
Key distribution
Public/Private keys

RSA Digital signature



Demonstrate RSA symmetry

Encryption with **e** & Decryption with **d**

$C^d \bmod n = (P^e \bmod n)^d \bmod n$ — $C = P^e \bmod n$

$= P^{e\,d} \bmod n$ — $e\,d \bmod \phi(n) = 1 \;>>>\; e \times d = k\phi(n) + 1$

$= P^{k(\phi(n)+1} \bmod n$ — Euler-Fermat

$= P$

Encryption with **d** & Decryption with **e**

$C^e \bmod n = (P^d \bmod n)^e \bmod n$ — $C = P^d \bmod n$

$= P^{d\,x\,e} \bmod n$ — $d\,e \bmod \phi(n) = 1$

$= P^{k(\phi(n)+1} \bmod n$ — Euler-Fermat

$= P$

NORTHERN ARIZONA UNIVERSITY

Homework #3

Find an example with small numbers explaining RSA:

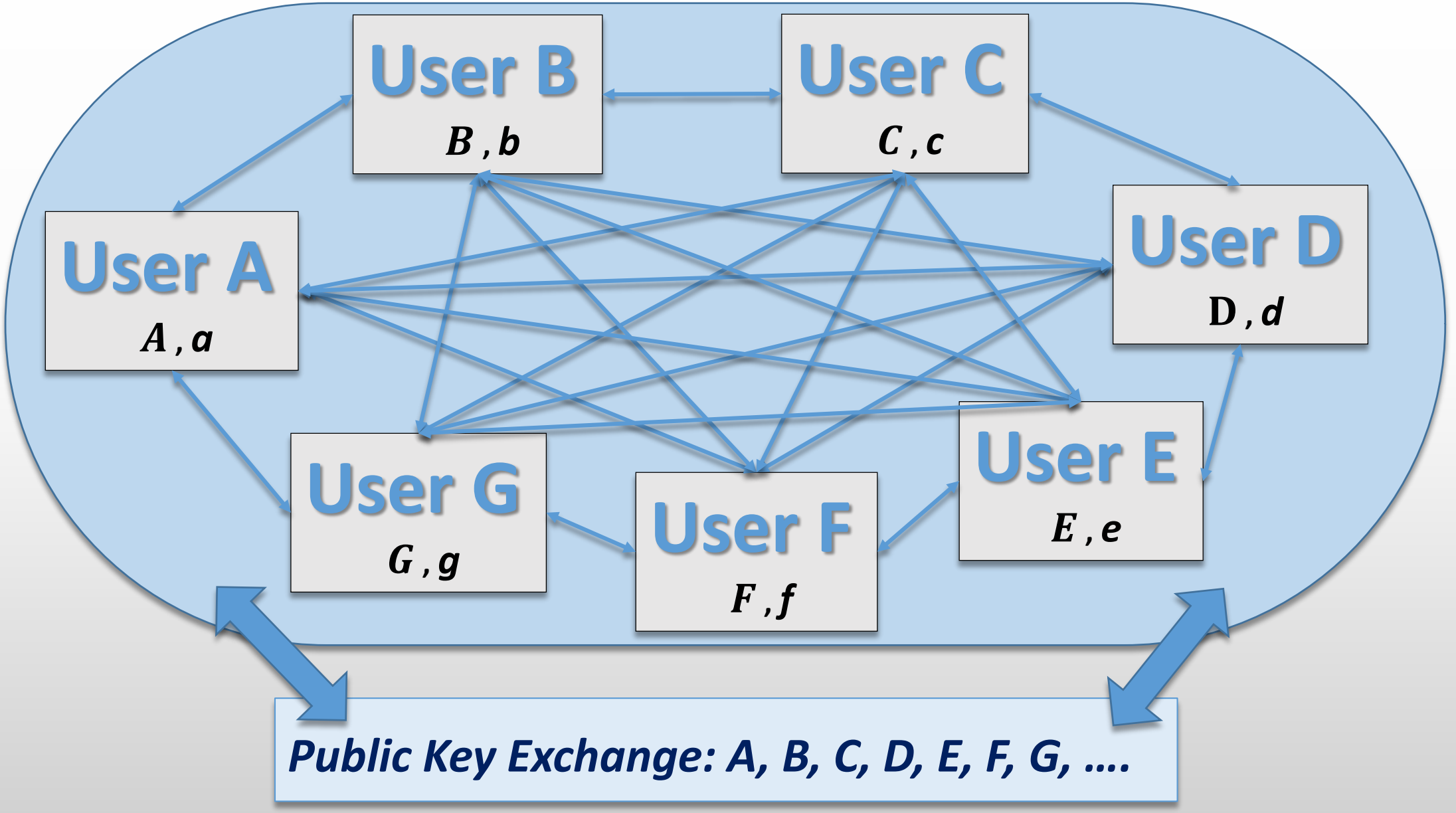
- Pick p and q prime below 15
- Calculate n
- Calculate $\phi(n)$
- Pick e
- Calculate the cipher of P=5
- Find back P

NORTHERN ARIZONA UNIVERSITY

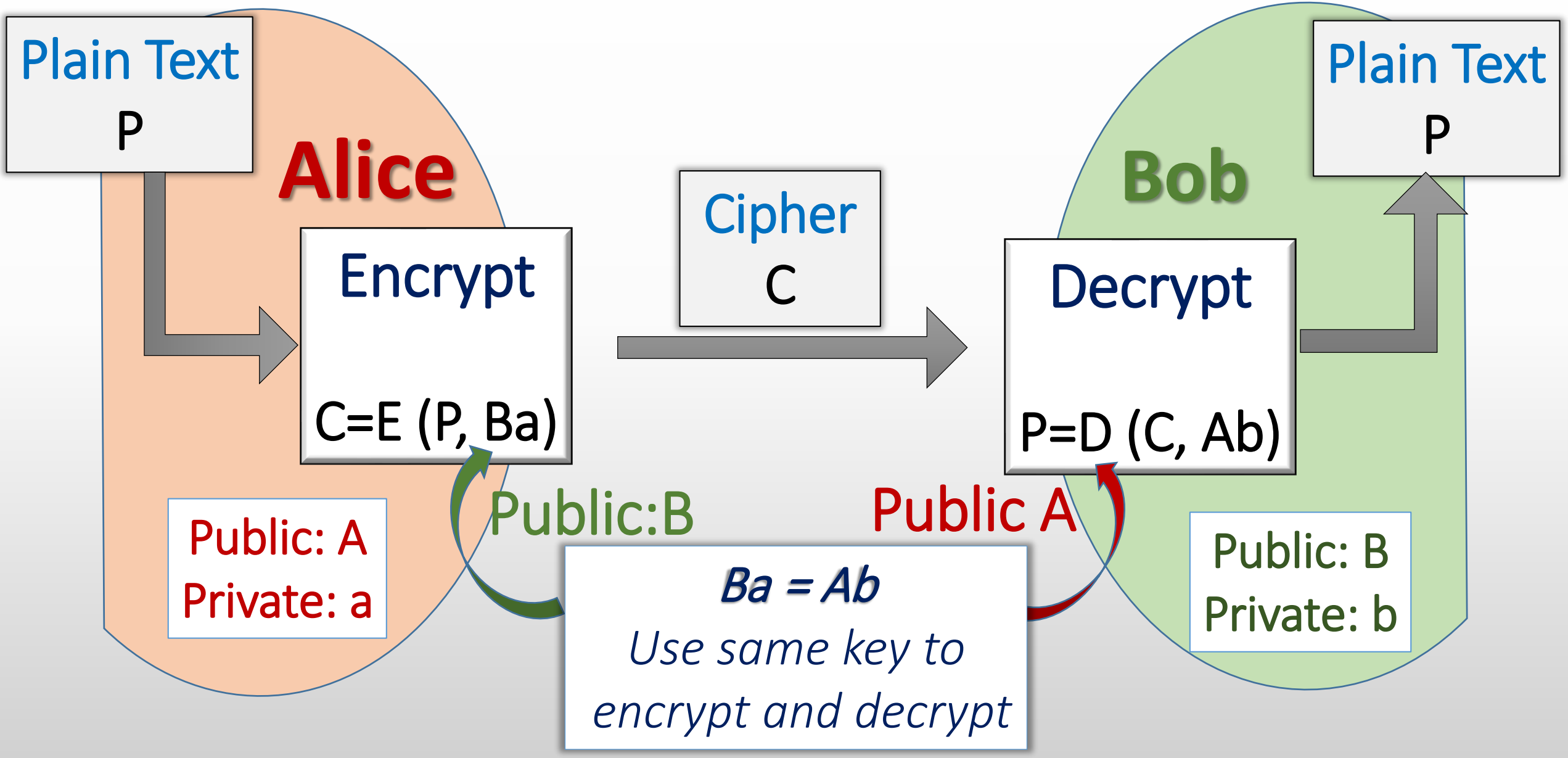
Public Key Infrastructure

- 1- Asymmetrical cryptography
- 2- Number theory
- 3- RSA
- 4- ECC

PKI with Elliptic Curve Cryptography (ECC)



Elliptic curve key exchange & encryption

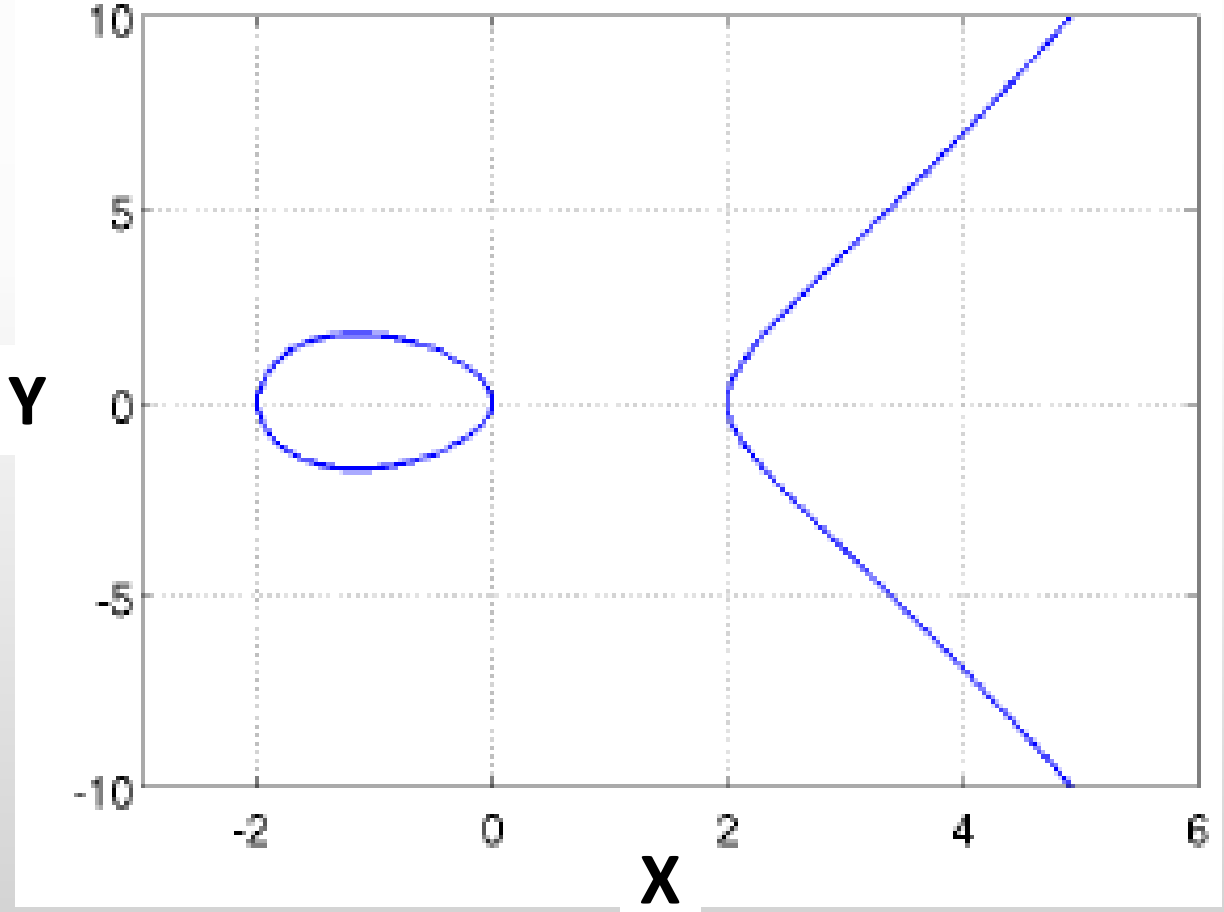


Elliptic Curves (EC) for cryptography

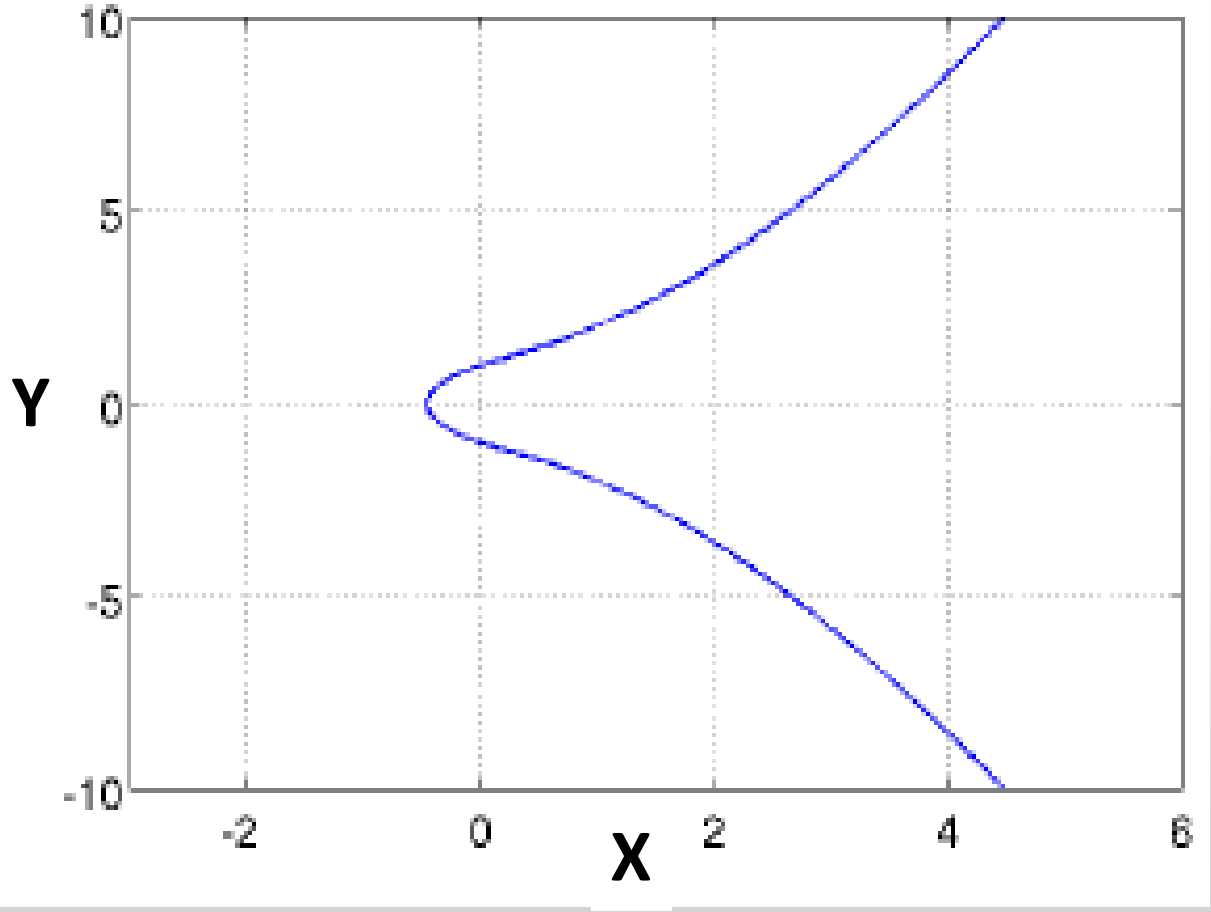
The set of all integer pairs (x, y, a, b) ϵ $\mathbb{Z}$ verifying: $y^2 = x^3 + a \cdot x + b$

(These elliptic curves are symmetric with the x axes: y_i and -y_i have the same x_i)

$y^2 = x^3 - 4 \cdot x + 0$



$y^2 = x^3 + 2 \cdot x + 1$



Definition of a circular finite ECC group G

The ECC group G is based on the modular group $\mathbb{Z}_m$

(m>3) is the set of all integer pairs (x, y) ∈ $\mathbb{Z}_m$ verifying:

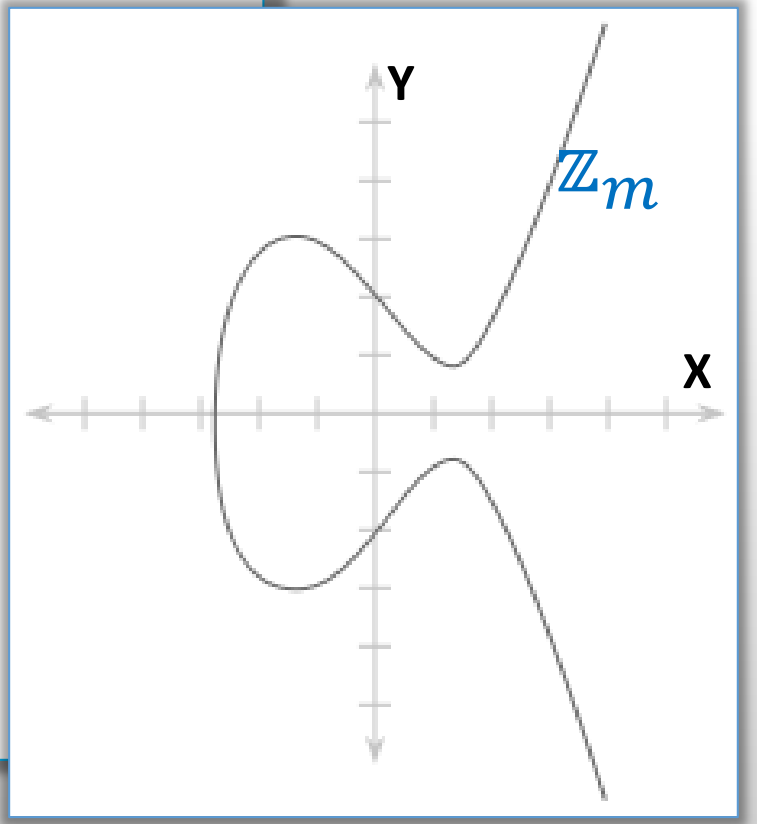
$$y^2 \equiv x^3 + a \,.\, x + b \bmod m$$

a, b ∈ $\mathbb{Z}_m$

$$4 \,.\, a^3 + 27 \,.\, b^2 \neq 0 \bmod m$$

The neutral is the point of infinity Θ

Ex: $y^2 \equiv x^3 - 3 \,.\, x + 3 \bmod m$



Arithmetic in the group operation (•) = "+" on ECC

Two elements:

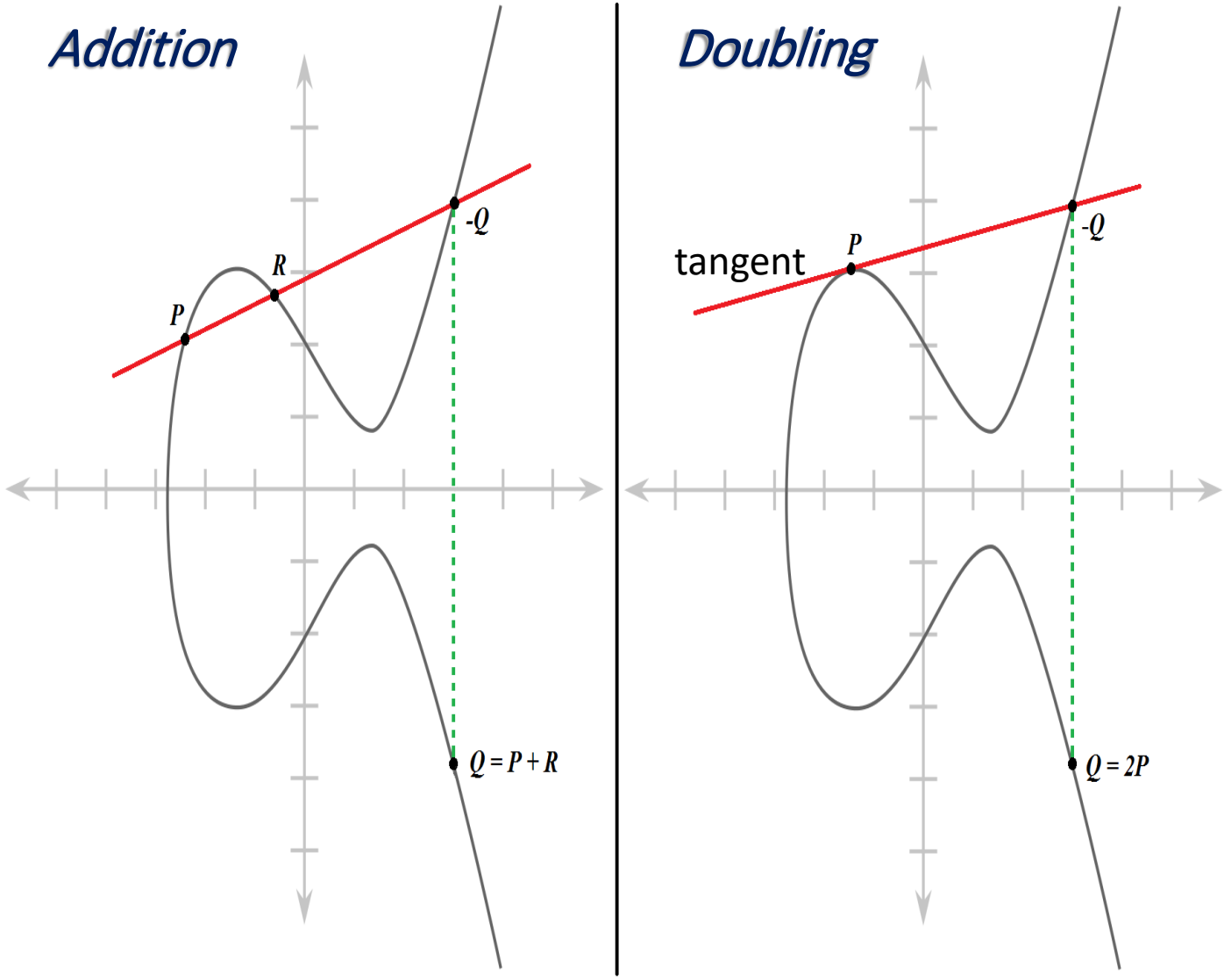
$P(x_1, y_1)$; $R(x_2, y_2) \in G$

Addition:

$P + R = Q$ $\quad Q(x_3, y_3)$

Point doubling:

$P + P = 2P = Q$



Formula: Point addition & doubling

$P = (x_1, y_1)$; $Q = (x_2, y_2)$; $R = (x_3, y_3)$

Point addition & doubling :

$$x_3 \equiv s^2 - x_1 - x_2 \bmod m$$

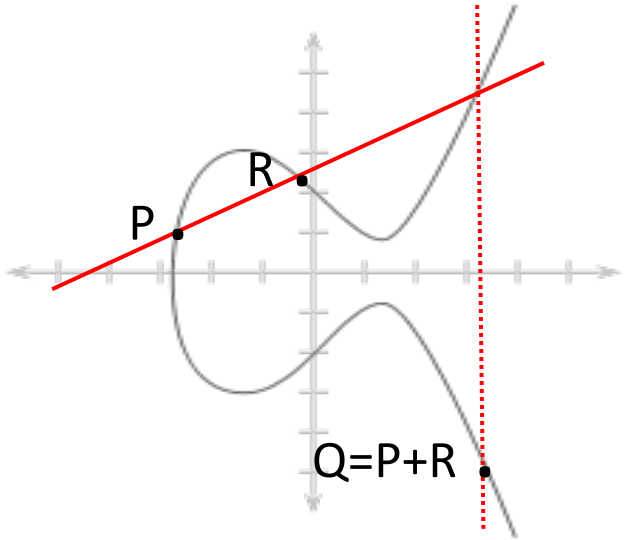
$$y_3 \equiv s\,(x_1 - x_3) - y_1 \bmod m$$

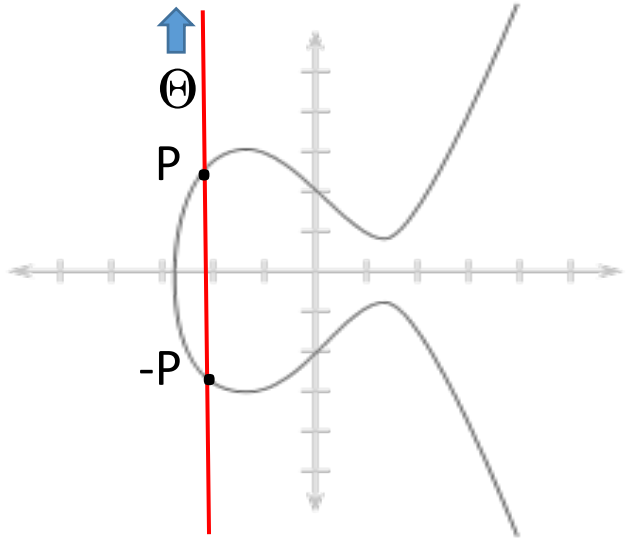
Where:

if $P \neq Q$ addition ➔ $s = (y_2 - y_1)\,(x_2 - x_1)^{-1} \bmod m$

if $P = Q$ doubling ➔ $s = (3x_1^2 + a)\,(2\,y_1)^{-1} \bmod m$

s is the slope of the EC





Neutral: $P + \Theta = P$

Inverse: $P + (-P) = \Theta$

$P = (x_1, y_1)$ => $(-P) = (x_1, -y_1)$

Example: Point doubling

We consider the small group $\mathbb{Z}_{17}$ => E: $y^2 \equiv x^3 + 2x + 2 \bmod 17$

We want to double the point **P = (5, 1)** => 2 P = (5, 1) + (5, 1)

$$s = (3x_1^2 + a)(2\ y_1)^{-1} = (75 + 2)(2)^{-1} \equiv 9 \cdot 9 \bmod 17 \equiv 13 \bmod 17$$

$$x_3 \equiv s^2 - x_1 - x_2 = 159 \equiv 6 \bmod 17$$

$$y_3 \equiv s(x_1 - x_3) - y_1 = 13(5 - 6) - 1 = -14 \equiv 3 \bmod 17$$

2 P = (6, 3)

This point is actually on the EC curve:

$$y^2 \equiv x^3 + 2x + 2 \bmod 17$$

$$3^2 \equiv 6^3 + 2 \cdot 6 + 2 \bmod 17$$

Creation of cyclic subgroup from EC

Theorem:

The points on an elliptic curve together with Θ have elliptic subgroups.
Under certain conditions all points on an elliptic curve form a cyclic group.

Example:

E: $y^2 \equiv x^3 + 2x + 2 \bmod 17$

Primitive element: P = (5, 1), the order is $\#E = 19$

2 P = (6, 3)
3 P = (10, 6)
4 P = (3, 1)
5 P = (9, 16)
6 P = (16, 13)
7 P = (0, 6)
8 P = (13, 7)
9 P = (7, 6)
10 P = (7, 11)
11 P = (13, 10)
12 P = (0, 11)
13 P = (16, 4)
14 P = (9, 1)
15 P = (3, 16)
16 P = (10, 11)
17 P = (6, 14)
18 P = (5, 16) = (-P)
19 P = Θ

Hasse's Theorem:

Given an EC E modulo m, the number of points on the curve denoted by $\#E$ is bounded by:

$$m + 1 - 2\sqrt{m} \leq \#E \leq m + 1 + 2\sqrt{m}$$

Proof:
18 P = (5, 16) = (5, -1) = (-P)
-1 = 16 mod 17

EC Discrete Logarithm Problem (ECDLP)

Definition:

Given a cycling subgroup E of an elliptic curve we consider a primitive element *P*, and another element *T*.

The problem is finding integer *d*, where: $1 \leq d \leq \#E$

$$\underbrace{P + P + \ldots\ldots + P}_{d \text{ times}} = d \,.\, P = T = (x_T, y_T)$$

In cryptography systems:

d is the private key, and $T = (x_T, y_T)$ is the public key

$$T = d \,.\, P$$

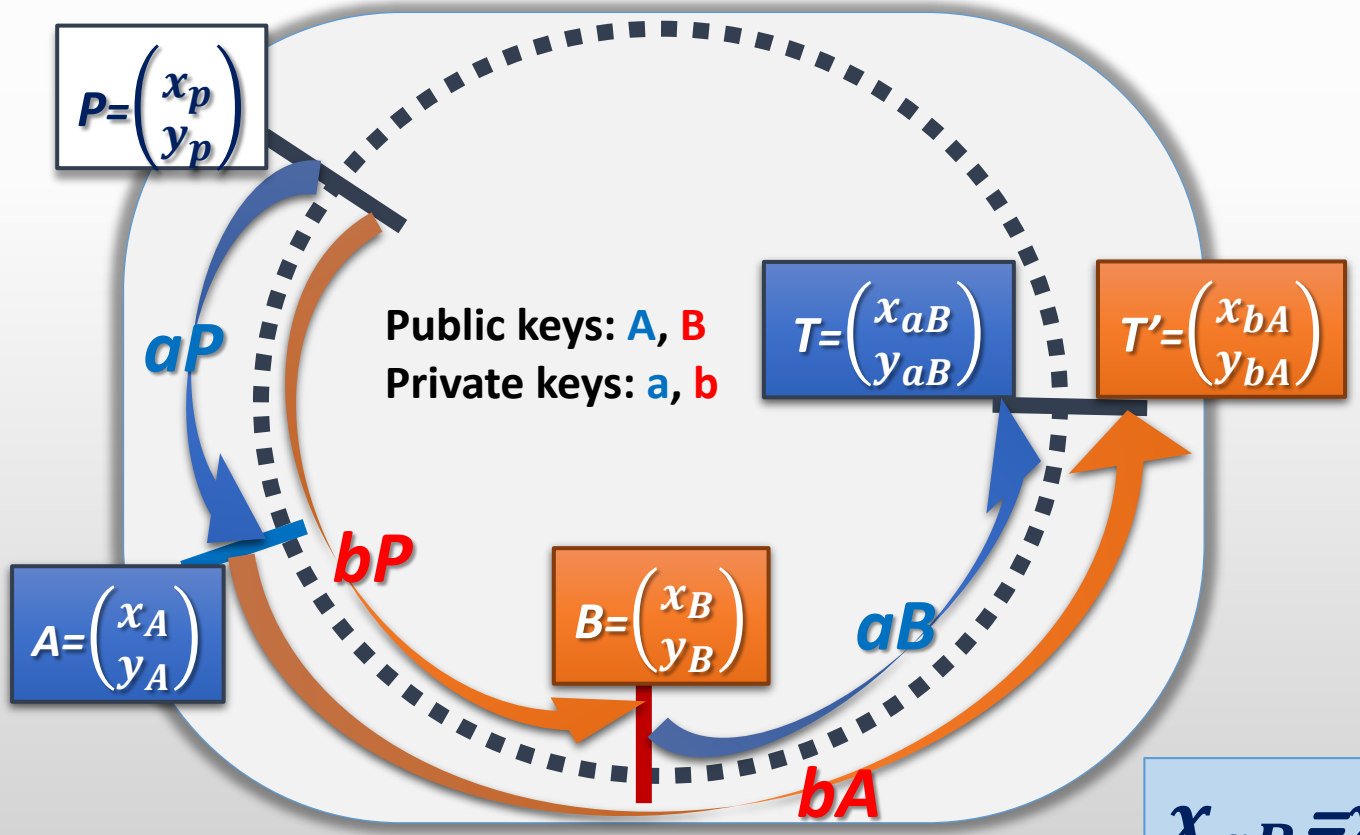
Ex: P (5,1) T(16, 4) ➔ d=13

EC Diffie-Hellman Key Exchange (ECDHKE)

1- Choose a prime P and the elliptic curve E $y^2 \equiv x^3 + \alpha \,.\, x + \beta \; mod\, m$

2- Chose a primitive element $P = (x_P, y_P)$

This give a domain with $\#E$ integers in the cyclic group having separate pairs



A encrypt with AES using x_{aB} as a key

B decrypt with AES using x_{bA} as a key

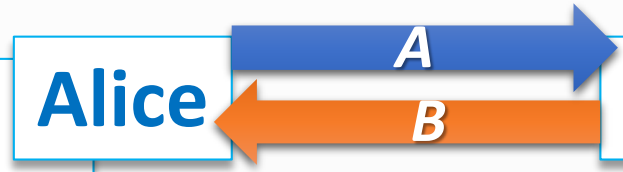
$x_{aB} = x_{bA}$ Proof: aB=a(bP)=(ab)P=b(aP)=bA

EC Diffie-Hellman Key Exchange (ECDHKE)

1- Choose a prime P and the elliptic curve E $\quad y^2 \equiv x^3 + \alpha \,.\, x + \beta \; mod\, m$

2- Chose a primitive element $\quad P = (x_P, y_P)$

This give a domain with $\#E$ integers in the cyclic group having separate pairs



Key Exchange:

Choose a private key

$P_{PrivA} = a \;\; \epsilon \{2, 3, \dots, \#E\text{-}1\}$

Calculate a public key

$P_{PubA} = A = a\,P = (x_A, y_A)$

Key Exchange:

Choose a private key

$P_{PrivB} = b \;\; \epsilon \{2, 3, \dots, \#E\text{-}1\}$

Calculate a public key

$P_{PubB} = B = b\,P = (x_B, y_B)$

Cryptography: Compute aB

$T_{AB} = (x_{AB}, y_{AB})$

Encrypt with AES using the key x_{AB}

Cryptography: Compute Ba

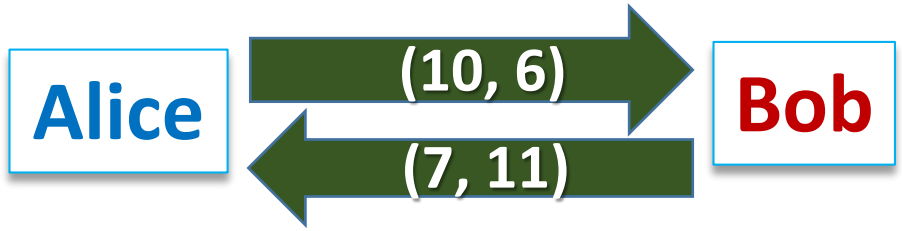
$T_{BA} = (x_{BA}, y_{BA})$

Decrypt with AES using the key x_{BA}

Example of key exchange

Group E defined by the following EC: $y^2 \equiv x^3 + 2x + 2 \bmod 17$

Base P = (5, 1) #E = 19



Private key $P_{PrivA} = a = 3$

Public key $P_{PubA} = A = 3\ P = (10, 6)$

Compute:

$aB = T_{AB} = 3\ (7, 11) = (13, 10)$

Private key $P_{PrivB} = b = 10$

Public key $P_{PubB} = B = 10\ P = (7, 11)$

Compute:

$bA = 10(10, 6) = (13, 10)$

(3 x 10) P = 30 P = 30-19 P = 11P

Encrypt with AES using 13 as a key

Decrypt with AES using 13 as a key

NORTHERN ARIZONA UNIVERSITY

Homework #4

Find a different example with different public keys, same cyclic group

- Pick the base, and private keys ***a*** and ***b***
- Calculate public keys **A** and **B**
- Calculate ***a*****B** and ***b*****A**
- Extract the common key

Benchmark

CPU Ticks for various key generation methods

RSA	CPU Ticks	ECC GF(P)	CPU Ticks	ECC GF(2^N)	CPU Ticks
1024	*23,443*				
2048	*59,845*	*128*	*313*	*113*	*981*
3072	*417,166*	*256*	*1,204*	*233*	*4,393*
4096	*1,492,687*	*521*	*4,696*	*409*	*12,294*

Benchmark

Protection against quantum computers

Algorithm	Key Length	Eq. security level (conventional)	Eq. security level (quantum computing)
RSA-1024	*1024 bits*	*80 bits*	*0 bits*
RSA-2048	*2048 bits*	*112 bits*	*0 bits*
ECC-256	*256 bits*	*128 bits*	*0 bits*
ECC-384	*384 bits*	*192 bits*	*0 bits*
AES-256	*256 bits*	*128 bits*	*128 bits*

NSA dreams of quantum computer that can break encryption

Spy agency is apparently not close to a quantum breakthrough, but it's trying.

by **Jon Brodkin** - Jan 2, 2014 3:34pm PST

The National Security Agency is conducting what it calls "basic research" to determine whether it's possible to build a quantum computer that would be useful for breaking encryption. The news isn't surprising—it would be surprising if the NSA *wasn't* researching quantum computing given the measures it's taken to undermine encryption standards used to protect Internet communications. The NSA's quantum work was described in documents leaked by Edward Snowden and published today in the *Washington Post*. A three-page NSA document describes a project to conduct "basic research in quantum physics and architecture/engineering studies to determine if, and how, a cryptologically useful quantum computer can be built."

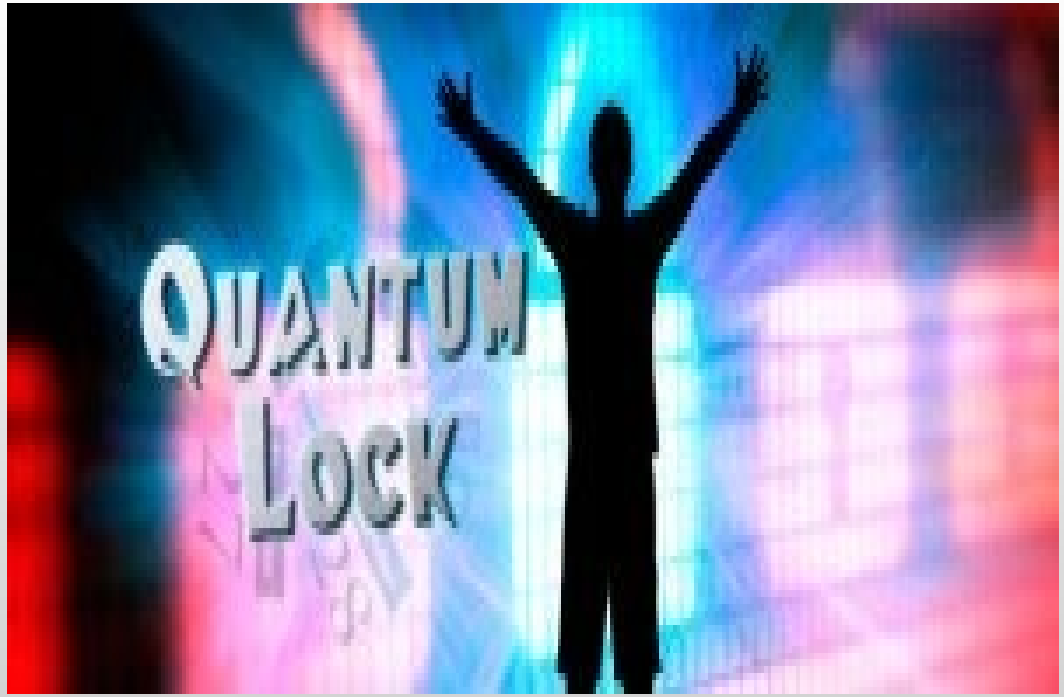
This is part of a $79.7 million research program called "Penetrating Hard Targets." A project goal for fiscal 2013 was to "Demonstrate dynamical decoupling and complete quantum control on two semiconductor qubits," the basic building block of a large-scale quantum computer. The NSA description of the program says the agency will "[c]ontinue research of quantum communications technology to support the development of novel Quantum Key Distribution (QKD) attacks and assess the security of new QKD system designs."

QUANTUM CRYPTOGRAPHY: YESTERDAY, TODAY, AND TOMORROW

Does it have a future? Classic cryptology isn't budging, but all depends on QKD. There's nothing specific enough in the NSA document to conclude that the agency is any more advanced in its quantum computing research than the rest of the scientific community. “It seems improbable that the NSA could be that far ahead of the open world without anybody knowing it,” MIT Professor of Electrical Engineering and Computer Science Scott Aaronson told the *Post*.

Some of the NSA's experiments are carried out "in large, shielded rooms known as Faraday cages, which are designed to prevent electromagnetic energy from coming in or out," the *Post* wrote. "Those, according to one brief description, are required 'to keep delicate quantum computing experiments running.'" The article noted that "the NSA appears to regard itself as running neck and neck with quantum computing labs sponsored by the European Union and the Swiss government" but has no hopes of an "immediate breakthrough.“

Another NSA document describing why the agency has classified its research says it's hoping to devise ways to protect US systems against quantum attack. While the NSA wants to "develop cryptanalytic QC [quantum computers] to attack high-grade public key encryption systems," it also seeks "to protect our own systems against adversarial cryptanalytic QC efforts."



NORTHERN ARIZONA UNIVERSITY®

QUESTIONS ?

Dr. Bertrand Cambou
Professor of Practice NAU, Cybersecurity
School of Informatics, Computing, and Cyber-Systems
Bertrand.cambou@nau.edu